

UNITED STATES DISTRICT COURT

for the
Southern District of West VirginiaIn the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*iPhone of GRACYN COURTRIGHT located at the FBI
Charleston Resident Agency Office, 113 Virginia Street,
East, Charleston, West Virginia 25301

Case No. 2:21-mj-00010

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Southern District of West Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC §§1752(a)(1) and (2) ;	entry of restricted building; disruption of Government business; disorderly conduct
40 USC §§ 5014(e)(2)(D) and	within the U.S. Capitol; parade, demonstrate, or picket within a Capitol building;
(G); and 18 USC § 641	and theft of government property

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

 Applicant's signature

Mariam Hanna, Special Agent

Printed name and title
FBIAttested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone and email *(specify reliable electronic means)*.Date: 01/21/2021

 Judge's signature
City and state: Charleston, West Virginia

Dwane L. Tinsley, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Property to be searched

One iPhone surrendered by Gracyn Courtright at her arrest on January 19, 2021 and currently in the custody of the Federal Bureau of Investigation (FBI) at the Charleston Resident Agency Office located at 113 Virginia Street, East, Charleston, West Virginia 25301. The iPhone is light gold in color with a cracked screen.



ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of Title 18 U.S.C. § 1752(a)(1) and (2), 40 U.S.C. § 5104(e)(2)(D) and (G), 18 U.S.C. § 641, 18 U.S.C. § 2101; 18 U.S.C. § 1512, and other related offenses as described in the search warrant affidavit, existing on the iPhone described in Attachment A including, but not limited to:

- a. Records or information regarding travel and lodging to and from the Washington, D.C. area from January 1, 2021, to present;
- b. Records and information that constitute evidence of the state of mind of COURTRIGHT, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;
- c. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with COURTRIGHT about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
- d. Evidence of COURTRIGHT's connection to the social media accounts described in the affidavit;

- e. Photographs or videos depicting COURTRIGHT or others entering the United States Capitol building, their activities prior to entry, during their occupancy of the premises, and upon exiting the premises;
- f. Electronic messages in whatever format (e.g. text messages, instant messages, messaging facilitated by applications being run on the iPhone) that remain stored within the electronic memory of the iPhone;
- g. Evidence of who used, owned, or controlled the iPhone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- h. Evidence of software, or the lack thereof, that would allow others to control the iPhone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- i. Evidence of the attachment to the iPhone of other storage devices or similar containers for electronic evidence;
- j. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the iPhone;
- k. Evidence of the times the iPhone was used;
- l. Passwords, encryption keys, and other access devices that may be necessary to access the iPhone;

- m. Records of or information about Internet Protocol addresses used by the iPhone;
- n. Records of or information about the iPhone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

In aid of the execution of the search of the iPhone described in Attachment A, law enforcement personnel are also specifically authorized to obtain from GRACYN COURTRIGHT the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock the iPhone to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of GRACYN COURTRIGHT.

While attempting to unlock the iPhone by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that GRACYN COURTRIGHT state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the iPhone. Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel GRACYN COURTRIGHT to state or otherwise provide that information. However, the voluntary disclosure of such information by GRACYN COURTRIGHT is permitted. To avoid confusion on that point, if agents in executing the warrant ask GRACYN COURTRIGHT for the password to the iPhone, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks the

iPhone, the agents will not state or otherwise imply that the warrant requires GRACYN COURTRIGHT to provide such information, and will make clear that providing any such information is voluntary and that she is free to refuse the request.

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA**

**IN THE MATTER OF THE SEARCH OF:
IPHONE OF GRACYN COURTRIGHT
LOCATED AT THE FBI CHARLESTON
RESIDENT AGENCY OFFICE, 113
VIRGINIA STREET, EAST,
CHARLESTON, WEST VIRGINIA 25301
UNDER RULE 41**

Case No. 2:21-mj-00010

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE**

I, Mariam Hanna, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search one light gold iPhone surrendered by GRACYN COURTRIGHT to the Federal Bureau of Investigation (FBI) on January 19, 2021, further described in Attachment A, for the things described in Attachment B.

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since January 2019. I am assigned to the Washington Field Office, and in addition to my regular duties I am currently tasked with investigating criminal activity in and around the Capitol grounds.

3. As a Special Agent, I am a "Federal law enforcement officer" within the meaning of Fed. R. Crim. P. 41 (a)(2)(C) and am authorized to execute warrants issued under the authority of the United States.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that GRACYN COURTRIGHT has committed violations of 18 U.S.C. §§ 1752(a)(1) and (a)(2), which makes it a crime to (1) knowingly enter or remain in any restricted building or grounds without lawful authority to do so; (2) knowingly, and with intent to impede or disrupt the orderly conduct of Government business or official functions, engage in disorderly or disruptive conduct in, or within such proximity to, any restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of Government business or official functions; 40 U.S.C. § 5104(e)(2)(D), which makes it a crime to utter loud, threatening, or abusive language, or engage in disorderly or disruptive conduct, at any place in the Grounds or in any of the Capitol Buildings with the intent to impede, disrupt, or disturb the orderly conduct of a session of Congress; 40 U.S.C. § 5104(e)(2)(G), which makes it a crime to parade, demonstrate, or picket in any of the Capitol Buildings; and 18 U.S.C. § 641, which makes it a crime to embezzle, steal, purloin, or knowingly convert to his use or the use of another, ... a thing of value of the United States or of any department or agency thereof and there is probable cause to believe that evidence of these offenses is currently located within the memory of the iPhone more fully described in Attachments A and B. Additionally, based on my training and experience I respectfully submit

that there is probable cause to believe that evidence related to violations of 18 U.S.C. § 1512, which makes it a crime to corruptly otherwise obstruct, influence, or impede any official proceeding, or attempt or conspire to do so; 18 U.S.C. § 2101, which makes it a crime to travel in interstate or foreign commerce or use any facility of interstate or foreign commerce with intent to incite, organize, promote, encourage, participate in, carry on a riot, or commit any act of violence in furtherance of a riot, or to aid or abet any person in doing so; and related offenses, is currently located within the memory of the iPhone (also referenced herein as “device” or “electronic device”) more fully described in Attachments A and B.

PROBABLE CAUSE

Background: Events at the U.S. Capitol on January 6, 2021

6. The U.S. Capitol is secured 24 hours a day by U.S. Capitol Police. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by U.S. Capitol Police. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol. On January 6, 2021, the exterior plaza of the U.S. Capitol was also closed to members of the public.

7. On January 6, 2021, a joint session of the United States Congress convened at the United States Capitol, which is located at First Street, SE, in Washington, D.C. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting in separate chambers of the United States Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which had taken place on November

3, 2020. The joint session began at approximately 1:00 p.m. Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

8. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and U.S. Capitol Police were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

9. At such time, the certification proceedings were still underway, and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of the U.S. Capitol Police attempted to maintain order and keep the crowd from entering the Capitol; however, shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of the U.S. Capitol Police, as others in the crowd encouraged and assisted those acts.

10. Shortly thereafter, at approximately 2:20 p.m., members of the United States House of Representatives and United States Senate, including the President of the Senate and Vice President Mike Pence, were instructed to—and did—evacuate the chambers. Accordingly, the joint session of the United States Congress was effectively suspended until shortly after 8:00 p.m. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the sessions resumed.

11. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

Facts Specific to this Application

12. Following this incident, the FBI reviewed screenshots from an Instagram account under the account name @gracyn_dawn. This account name is consistent with COURTRIGHT's first and middle name. This account has since been deleted, so your affiant was unable to view the photographs on the Instagram page. However, the photographs that were posted were captured and provided to law enforcement via screenshots.

13. These screenshots appear to be photos taken on January 6, 2021, in Washington, D.C. and outside the Capitol. They are tagged with the location "Washington, D.C. Capital [sic] City." As seen in the first and second photographs below, an individual later identified as COURTRIGHT, is wearing a beanie-style hat with a yellow band, a black puffer-style jacket, a black shirt over a pink shirt, black pants, light pink socks, and a black fanny pack. Your affiant has viewed COURTRIGHT's West Virginia driver's license photo and the driver's license photograph (the third photo below) issued to COURTRIGHT, and the images below bear significant physical similarities, including hair color and facial structure, specifically dimples on both sides of the face.

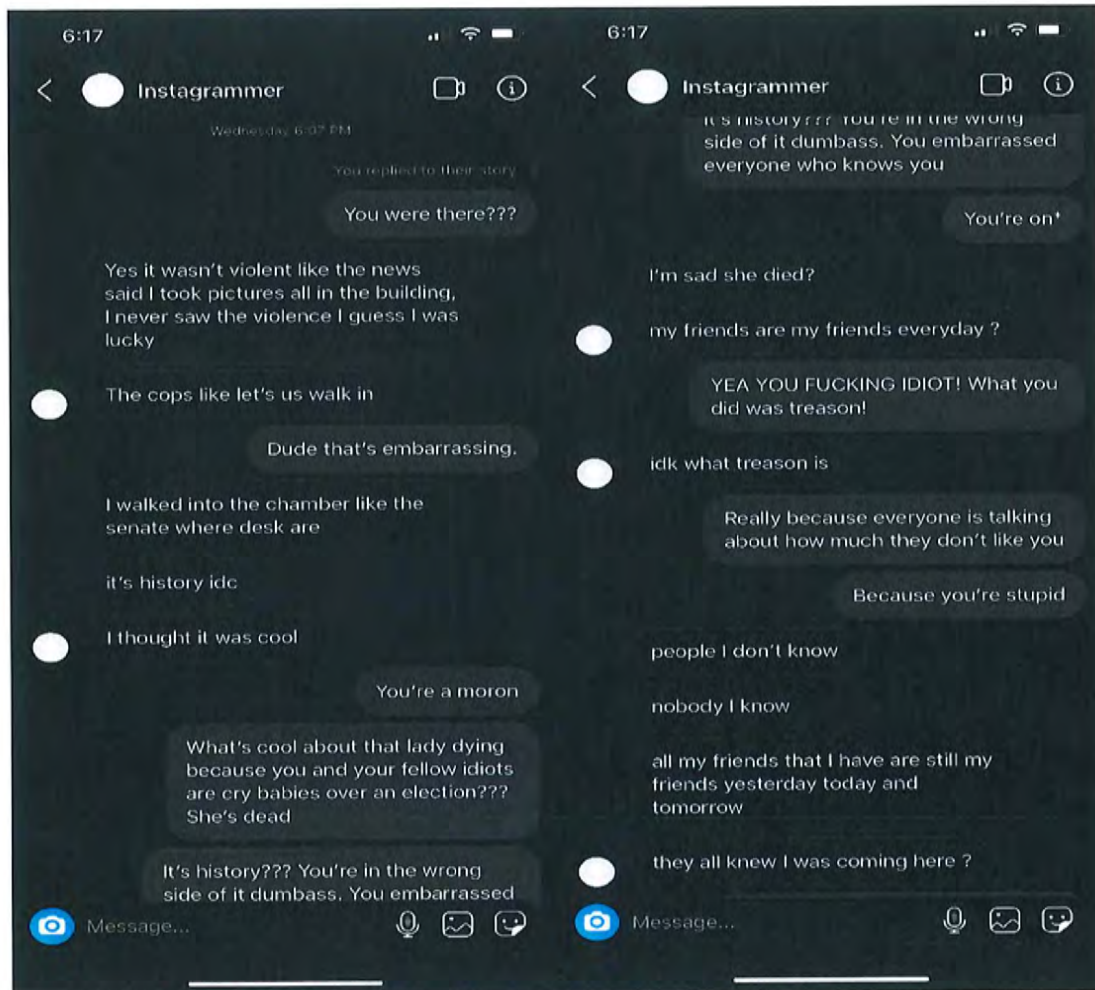


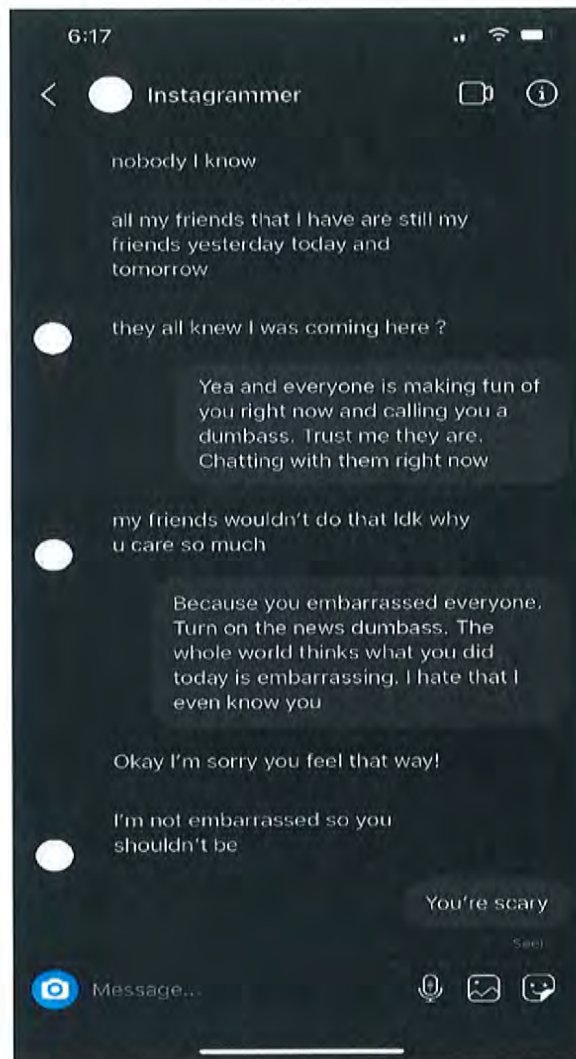


14. Another photograph posted to the Instagram account on or about January 6-7, 2021, shortly before her account was deactivated, also shows COURTRIGHT with the quote “Infamy is just as good as fame. Either way I end up more known. XOXO.” The iPhone described in Attachment A can be seen in the photograph.



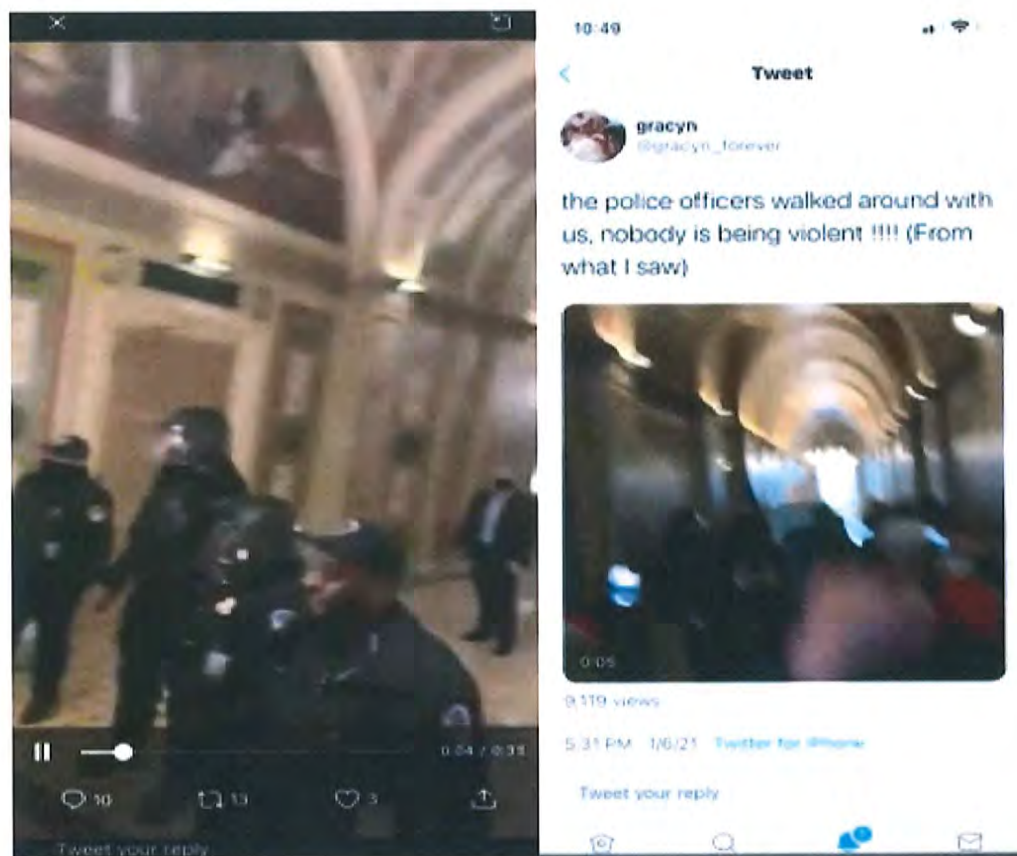
15. The FBI was also provided with screenshots of a private or “direct message” between COURTRIGHT and Witness 1 (W1) on Instagram. After viewing a video of COURTRIGHT chanting through the halls of the Capitol, W1 messaged COURTRIGHT to ask if she was there. COURTRIGHT responded that she walked into “the chamber like the senate where desks are [sic]” and that she “took pictures all in the building.”

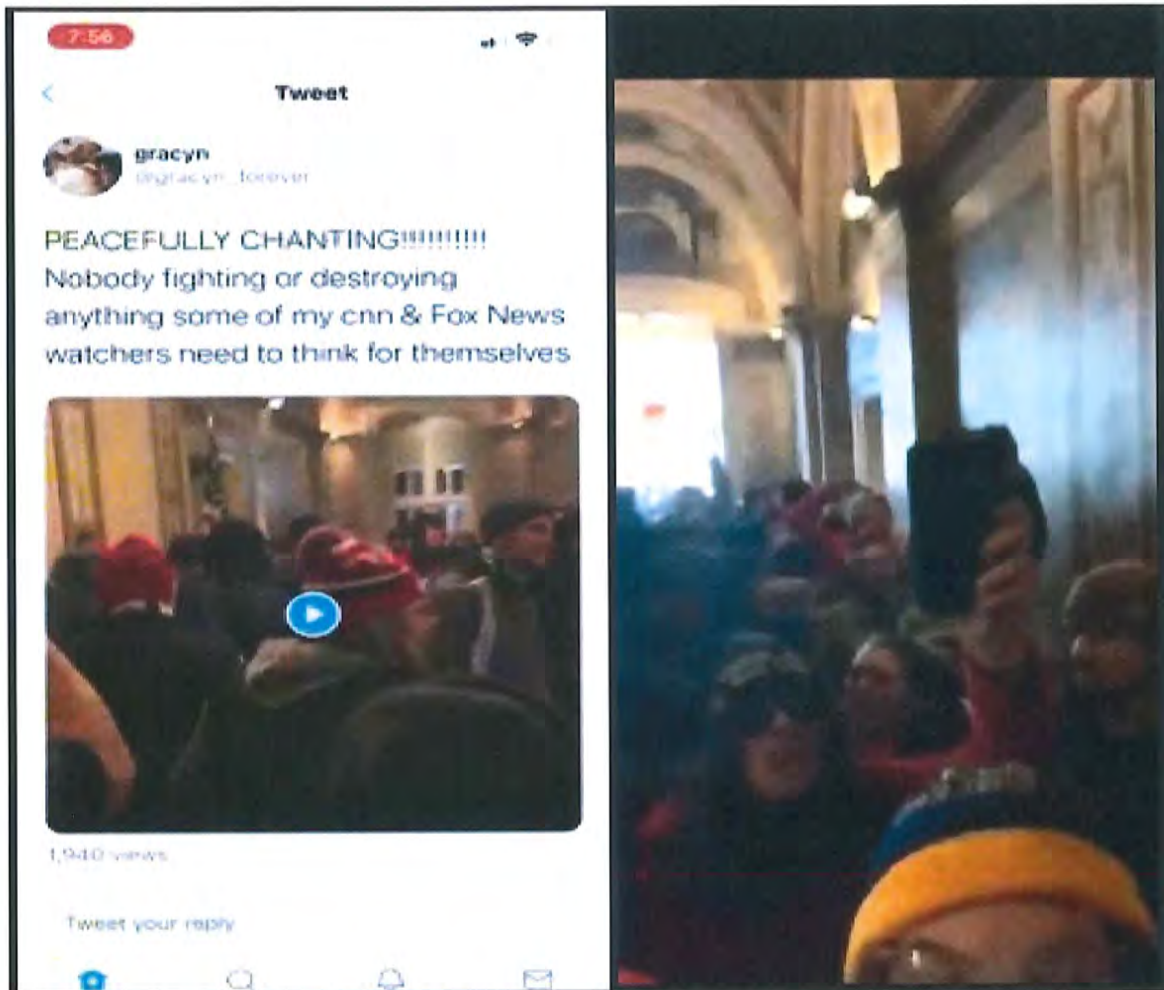




16. In addition to the posts on Instagram, the FBI also reviewed photos and videos posted to a Twitter account with an account name of "gracyn_forever." The account name is consistent with COURTRIGHT's first name. As with the Instagram account, this account has since been deleted, so your affiant was unable to view the photographs or videos on Twitter. However, photographs and videos posted on the account were captured and provided to law

enforcement. Screenshots from these videos are below. These videos appear to be filmed by COURTRIGHT, and at one point she turns the camera towards herself and the yellow band of the hat depicted above is clearly visible. One video shows her with a crowd inside the Capitol chanting “USA.” Another video shows her and others approaching a line of law enforcement officers inside the Capitol chanting “whose house, our house.”





17. Additionally, a photo published by the Washington Post (attached below) appears to show COURTRIGHT in a crowd that initially clashed with police in the halls of the Capitol. The FBI has determined that the video COURTRIGHT had personally taken and posted was taken during approximately the same time that this photo was captured. COURTRIGHT can be identified by her unique hat with the yellow band, the surrounding people, flag, and building

architecture (all of which can be seen in both this picture and her personally captured video).

The iPhone more fully described in Attachment A can also be seen in the photograph.



18. Capitol Police reviewed surveillance footage from January 6, 2021, located COURTRIGHT, and provided the footage to your affiant. COURTRIGHT was seen entering the Capitol building via a door near the West Senate Stairs at 2:42 p.m.. This is the same hallway depicted in the photos and videos provided to law enforcement. When entering the Capitol building she can be seen stepping over broken glass and individuals around her are attempting to break down doors. At 3:01 p.m., COURTRIGHT can be seen on the second floor, walking up the steps near the Senate Chamber and room S214 carrying a “Members Only” sign (photo below).

She was not seen entering the Senate Chamber. A few minutes later, at 3:05 p.m., she can be seen on the second floor near S208. At this point, a law enforcement officer takes the “Members Only” sign away from her. COURTRIGHT leaves the building through the North Door at 3:06 p.m.





19. On January 10, 2021, the FBI found a University of Kentucky news article on kykernal.com titled, “*‘Infamy is just as good as fame’: UK student among crowd that mobbed Capitol building,*” which detailed her involvement in the riots. COURTRIGHT is a senior at the University of Kentucky.

20. On January 12, 2021, an FBI Agent telephonically interviewed COURTRIGHT’s father, who indicated she was staying with him at his home in West Virginia. He acknowledged her involvement in the Capitol riots and stated that she would cooperate with law enforcement.

21. On January 14, 2021, FBI Special Agents went to COURTRIGHT’s father’s residence in Hurricane, West Virginia to interview COURTRIGHT. COURTRIGHT’s father indicated that he did not feel comfortable allowing COURTRIGHT to give a statement unless

she was notified she would not get in trouble for her actions.¹ However, he told the FBI that COURTRIGHT traveled to Washington, D.C., to be at “the party” and stayed with friends from high school who live in the Washington D.C. area. According to her father, she was in the front of the crowd during President Donald TRUMP’s speech. Her father further stated that she made it to the Capitol an hour after TRUMP gave his speech, and she did not remember which side of the Capitol she was on when she entered the building. Her father stated that she had recalled walking up a ramp prior to entering the Capitol and was able to walk in. The father concluded by stating that if his daughter was charged with a crime, he would assist in ensuring she turned herself in to authorities.

22. Based on the forgoing, your affiant respectfully submits that there is probable cause to believe that GRACYN COURTRIGHT has committed violations of 18 U.S.C. §§ 1752(a)(1) and (a)(2), which makes it a crime to (1) knowingly enter or remain in any restricted building or grounds without lawful authority to do so; (2) knowingly, and with intent to impede or disrupt the orderly conduct of Government business or official functions, engage in disorderly or disruptive conduct in, or within such proximity to, any restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of Government business or official functions; 40 U.S.C. § 5104(e)(2)(D), which makes it a crime to utter loud, threatening, or abusive language, or engage in disorderly or disruptive conduct, at any place in the Grounds

¹ COURTRIGHT’s father represented that he was a lawyer, but was not COURTRIGHT’S criminal attorney, and that if she was charged with anything, a separate attorney would be hired for her.

or in any of the Capitol Buildings with the intent to impede, disrupt, or disturb the orderly conduct of a session of Congress; 40 U.S.C. § 5104(e)(2)(G), which makes it a crime to parade, demonstrate, or picket in any of the Capitol Buildings; and 18 U.S.C. § 641, which makes it a crime to embezzle, steal, purloin, or knowingly convert to his use or the use of another, ... a thing of value of the United States or of any department or agency thereof and there is probable cause to believe that evidence of these offenses is currently located within the memory of the iPhone more fully described in Attachments A and B. Additionally, your affiant further submits that there is probable cause to believe that evidence related to violations of 18 U.S.C. § 1512, which makes it a crime to corruptly otherwise obstruct, influence, or impede any official proceeding, or attempt or conspire to do so; 18 U.S.C. § 2101, which makes it a crime to travel in interstate or foreign commerce or use any facility of interstate or foreign commerce with intent to incite, organize, promote, encourage, participate, in, carry on a riot, or commit any act of violence in furtherance of a riot, or to aid or abet any person in doing so; and related offenses, is currently located within the memory of the iPhone (also referenced herein as “device” or “electronic device”) more fully described in Attachments A and B.

23. On January 16, 2021, COURTRIGHT was charged with the offenses described above in a criminal complaint filed in the United States District Court for the District of Columbia (Case No. 1:21-mj-0082). An arrest warrant was issued, and COURTRIGHT surrendered herself to the FBI in Charleston, West Virginia. At the time of her arrest, COURTRIGHT surrendered the iPhone described in Attachment A. The iPhone remains in the

custody of the FBI at the Charleston Resident Agency Office located at 113 Virginia Street, East, Charleston, West Virginia 25301.

TECHNICAL TERMS

24. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Digital device,” as used herein, includes the following three terms and their respective definitions:

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not

limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking,

sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives

signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is,

long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A “modem” translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file’s hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. “VPN” means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive

data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network—hence the name “virtual private network.” The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. “Malware,” short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

25. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the iPhone described in Attachment A. Thus, the warrant applied for would authorize the seizure of the device or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that based on the nature of smartphones, there is probable cause to believe that the items described in Attachment B will be stored in the electronic memory of the iPhone for at least the following reasons:

a. Individuals who engage in criminal activity, including documenting illegal activity, communicating with co-conspirators online; storing on digital devices, like the iPhone, documents, photos, videos, and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social media accounts.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smartphone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smartphone, or other digital device habits.

26. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes

described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device was used, the purpose of its use, who used it (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be on the iPhone because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the device, not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords.

Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smartphone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team

and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to plan and document illegal activity, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

27. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other

digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering

most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

28. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the iPhone.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching

the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC ACCESS TO DEVICE(S)

29. This warrant permits law enforcement agents to obtain from the person of GRACYN COURTRIGHT the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the iPhone. The grounds for this request are as follows:

30. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

31. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors

found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

32. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

33. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

34. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in

some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

35. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event the iPhone is locked and equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

36. Due to the foregoing, if the iPhone is locked and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s); (2) hold the iPhone in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the iPhone in

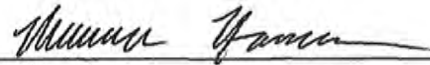
front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the iPhone in order to search its contents as authorized by this warrant.

The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

37. I submit that this affidavit supports probable cause for a warrant to search the iPhone described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,



Mariam Hanna
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on by Telephone or Other Reliable Electronic Means on January 21st, 2021.



DWANE L. TINSLEY,
UNITED STATES MAGISTRATE JUDGE